SOPHOS

Sophos Anti-Virus for UNIX and Linux
user manual

Product version: 4
Document date: January 2011

Contents

1 About this manual....3
2 About Sophos Anti-Virus for UNIX and Linux....4
3 On-demand scanning....5
4 What happens if viruses are detected....9
5 Cleaning up viruses....10
6 Appendix A: On-demand scan return codes....13
7 Troubleshooting....15
8 Technical support....20
9 Legal notices....21

1 About this manual

This manual tells you how to use and configure Sophos Anti-Virus for UNIX and Linux.

To install Sophos Anti-Virus on standalone and networked UNIX and Linux computers, see the *Sophos Anti-Virus for UNIX and Linuxstartup guide* for version 4.

To install Sophos Anti-Virus so that it is updated automatically by Sophos Enterprise Console, see the *Sophos Endpoint Security and Control startup guide for Linux, NetWare, and UNIX*.

Sophos documentation is published at *www.sophos.com/support/docs/*.

2 About Sophos Anti-Virus for UNIX and Linux

2.1 What Sophos Anti-Virus does

Sophos Anti-Virus detects and deals with viruses (including worms and Trojans) on your UNIX or Linux computer. As well as being able to detect all UNIX and Linux viruses, it can also detect all other viruses that might be stored on your UNIX or Linux computer and transferred to other computers. It does this by scanning your computer.

2.2 How Sophos Anti-Virus protects your computer

Sophos Anti-Virus enables you to run an *on-demand scan*. An on-demand scan is a scan that you initiate. You can scan anything from a single file to everything on your computer that you have permission to read. You can either manually run an on-demand scan or schedule it to run unattended.

2.3 How you use Sophos Anti-Virus

Sophos Anti-Virus has a command-line interface. This enables you to access all the Sophos Anti-Virus functionality and to perform all configuration.

3 On-demand scanning

An *on-demand scan* is a scan that you initiate. You can scan anything from a single file to everything on your computer that you have permission to read. You can either manually run an on-demand scan or schedule it to run unattended.

To schedule an on-demand scan, use the command **crontab**. For details, see *Sophos support knowledgebase article 12176*.

3.1 Running on-demand scans

The command that you type to run an on-demand scan is **sweep**.

3.1.1 Scan the computer

- To scan the computer, type:
  sweep /

3.1.2 Scan a particular directory or file

- To scan a particular directory or file, specify the path of the item. For example, type:
  sweep /usr/mydirectory/myfile

  You can type more than one directory or file in the same command.

3.1.3 Scan a filesystem

- To scan a filesystem, specify its name. For example, type:
  sweep /home

  You can type more than one filesystem in the same command.

3.1.4 Scan a boot sector

Note: This applies only to Linux and FreeBSD.

To scan a boot sector, log in as superuser. This grants you sufficient permission to access the disk devices.

You can scan the boot sector of a logical or physical drive.

- To scan the boot sector of specific logical drives, type:
  sweep -bs=*drive*, *drive*, **...**

where *drive* is the name of a drive, for example /dev/fd0 or /dev/hda1.

- To scan the boot sector of all logical drives that Sophos Anti-Virus recognises, type:
  sweep -bs
- To scan the master boot record of all fixed physical drives on the computer, type:
  sweep -mbr

3.2 Configuring on-demand scans

In this section, where *path* appears in a command, it refers to the path to be scanned.

To see a full list of the options that you can use with an on-demand scan, type:

man sweep

3.2.1 Scan all file types

By default, Sophos Anti-Virus scans only executables. To see a full list of the file types that Sophos Anti-Virus scans by default, type **sweep -vv**.

- To scan all file types, not just those that are scanned by default, use the option **-all**. Type:
  sweep *path* **-all**

  Note: This makes scanning take longer, can compromise performance on servers, and can cause false virus reports.

3.2.2 Scan a particular file type

By default, Sophos Anti-Virus scans only executables. To see a full list of the file types that Sophos Anti-Virus scans by default, type **sweep -vv**.

- To scan a particular file type, use the option **-ext** with the appropriate filename extension. For example, to scan files that have the filename extension .txt, type:
  sweep *path* **-ext=txt**
- To disable scanning of a particular file type, use the option **-next** with the appropriate filename extension.

Note: To specify more than one file type, separate each filename extension with a comma.

3.2.3 Scan inside all archive types

You can configure Sophos Anti-Virus to scan inside all archive types. To see a list of these archive types, type **sweep -vv**.

- To scan inside all archive types, use the option **-archive**. Type:

sweep *path* **-archive**

Archives that are "nested" within other archives (for example, a TAR archive within a ZIP archive) are scanned recursively.

If you have numerous complex archives, the scan may take longer to run. Bear this in mind when scheduling unattended scans.

3.2.4 Scan inside a particular archive type

You can configure Sophos Anti-Virus to scan inside a particular archive type. To see a list of these archive types, type **sweep -vv**.

- To scan inside a particular archive type, use the option that is shown in the list. For example, to scan inside TAR and ZIP archives, type:
  sweep *path* **-tar -zip**

  Archives that are "nested" within other archives (for example, a TAR archive within a ZIP archive) are scanned recursively.

  If you have numerous complex archives, the scan may take longer to run. Bear this in mind when scheduling unattended scans.

3.2.5 Scan remote computers

By default, Sophos Anti-Virus does not scan items on remote computers (that is, does not traverse remote mount points).

- To scan remote computers, use the option **--no-stay-on-machine**. Type:
  sweep *path* **--no-stay-on-machine**

3.2.6 Turn off scanning of symbolically linked items

By default, Sophos Anti-Virus scans symbolically linked items.

- To turn off scanning of symbolically linked items, use the option **--no-follow-symlinks**. Type:
  sweep *path* **--no-follow-symlinks**

  To avoid scanning items more than once, use the option **--backtrack-protection**.

3.2.7 Scan the starting filesystem only

Sophos Anti-Virus can be configured not to scan items that are beyond the starting filesystem (that is, not to traverse mount points).

- To scan the starting filesystem only, use the option **--stay-on-filesystem**. Type:

sweep *path* **--stay-on-filesystem**

3.2.8 Excluding items from scanning

You can configure Sophos Anti-Virus to exclude particular items (files, directories, or filesystems) from scanning by using the option **-exclude**. Sophos Anti-Virus excludes any items that follow the option in the command string. For example, to scan items fred and harry, but not tom or peter, type:

sweep fred harry -exclude tom peter

You can exclude directories or files that are *under* a particular directory. For example, to scan all of Fred's home directory, but exclude the directory games (and all directories and files under it), type:

sweep /home/fred -exclude /home/fred/games

You can also configure Sophos Anti-Virus to *include* particular items that follow the option **-include**. For example, to scan items fred, harry, and bill, but not tom or peter, type:

sweep fred harry -exclude tom peter -include bill

3.2.9 Scan file types that UNIX defines as executables

By default, Sophos Anti-Virus does not scan file types that UNIX defines as executables.

- To scan file types that UNIX defines as executables, use the option **--examine-x-bit**. Type: **sweep** *path* **--examine-x-bit**

  Sophos Anti-Virus still scans files that have filename extensions that are in its own list as well. To see a list of these filename extensions, type **sweep -vv**.

4 What happens if viruses are detected

If an on-demand scan detects a virus, by default Sophos Anti-Virus displays a command-line alert. It reports the virus on the line which starts with >>> followed by either `Virus` or `Virus Fragment`:

```
SWEEP virus detection utility
Version 4.58.0 [Linux/Intel]
Virus data version 4.58, October 2010
Includes detection for 1375239 viruses, Trojans and worms
Copyright (c) 1989-2010 Sophos Group. All rights reserved.

System time 13:43:32, System date 22 September 2010

IDE directory is: /usr/savides/

Using IDE file nyrate-d.ide
. . . . . .
Using IDE file injec-lz.ide

Quick Scanning

>>> Virus 'EICAR-AV-Test' found in file /usr/mydirectory/eicar.src

33 files scanned in 2 seconds.
1 virus was discovered.
1 file out of 33 was infected.
Please send infected samples to Sophos for analysis.
For advice consult www.sophos.com or email support@sophos.com
End of Sweep.
```

For information about cleaning up viruses, see *Cleaning up viruses* (page 10).

5 Cleaning up viruses

5.1 Get cleanup information

If viruses are reported, you can get information and cleanup advice from the Sophos website.

To get cleanup information:

1. Go to the security analyses page (*www.sophos.com/security/analyses*).
2. Search for the analysis of the virus, by using the name that was reported by Sophos Anti-Virus.

5.2 Quarantining infected files

You can configure an on-demand scan to put infected files into quarantine to prevent them from being accessed. It does this by changing the ownership and permissions for the files.

Note: If you specify disinfection (see *Cleaning up infected files* (page 11)) as well as quarantining, Sophos Anti-Virus attempts to disinfect infected items and quarantines them only if disinfection fails.

In this section, where *path* appears in a command, it refers to the path to be scanned.

5.2.1 Specify quarantining

- To specify quarantining, use the option **--quarantine**. Type:
  sweep *path* **--quarantine**

5.2.2 Specifying the ownership and permissions that are applied

By default, Sophos Anti-Virus changes:

- The user ownership of an infected file to the user running Sophos Anti-Virus.
- The group ownership of the file to the group to which that user belongs.
- The file permissions to `-r--------` (0400).

If you prefer, you can change the user or group ownership and file permissions that Sophos Anti-Virus applies to infected files. You do so by using these parameters:

```
uid=nnn
user=username
gid=nnn
group=group-name
mode=ppp
```

You cannot specify more than one parameter for user ownership or for group ownership. For example, you cannot specify a **uid** *and* a **user**.

For each parameter that you do not specify, the default setting (as given earlier) is used.

For example:

sweep fred --quarantine:user=virus,group=virus,mode=0400

changes an infected file's user ownership to "virus", the group ownership to "virus", and the file permissions to `-r---------`. This means that the file is owned by the user "virus" and group "virus", but only the user "virus" can access the file (and only for reading). No-one else (apart from root) can do anything to the file.

You may need to be running as a special user or as superuser to set the ownership and permissions.

5.3 Cleaning up infected files

You can configure an on-demand scan to clean up (disinfect or delete) infected files. Any actions that Sophos Anti-Virus takes against infected files are listed in the scan summary and logged in the Sophos Anti-Virus log. By default, cleanup is disabled.

In this section, where *path* appears in a command, it refers to the path to be scanned.

5.3.1 Disinfect a specific infected file

- To disinfect a specific infected file, use the option **-di**. Type:
  sweep *path* **-di**

  Sophos Anti-Virus asks for confirmation before it disinfects.

  Note: Disinfecting an infected document does not repair any changes the virus has made to the document. (See *Get cleanup information* (page 10) to find out how to view details on the Sophos website of the virus's side-effects.)

5.3.2 Disinfect all infected files on the computer

- To disinfect all infected files on the computer, type:
  sweep / -di

  Sophos Anti-Virus asks for confirmation before it disinfects.

  Note: Disinfecting an infected document does not repair any changes the virus has made to the document. (See *Get cleanup information* (page 10) to find out how to view details on the Sophos website of the virus's side-effects.)

5.3.3 Delete a specific infected file

- To delete a specific infected file, use the option **-remove**. Type:
  sweep *path* **-remove**

  Sophos Anti-Virus asks for confirmation before it deletes.

5.3.4 Delete all infected files on the computer

- To delete all infected files on the computer, type:
  sweep / -remove

  Sophos Anti-Virus asks for confirmation before it deletes.

5.3.5 Disinfect an infected boot sector

Note: This applies only to Linux and FreeBSD.

- To disinfect an infected boot sector, use the disinfection option **-di** and the boot sector option **-bs**. For example, type:
  sweep -bs=/dev/fd0 -di

  where **/dev/fd0** is the name of the drive that contains the infected boot sector.

  Sophos Anti-Virus asks for confirmation before it disinfects.

5.4 Recovering from virus side-effects

Recovery from virus infection depends on how the virus infected the computer. Some viruses leave you with no side-effects to deal with; others may have such extreme side-effects that you have to restore a hard disk in order to recover.

Some viruses gradually make minor changes to data. This type of corruption can be hard to detect. It is therefore very important that you read the virus analysis on the Sophos website, and check documents carefully after disinfection.

Sound backups are crucial. If you did not have them before you were infected, start keeping them in case of future infections.

Sometimes you can recover data from disks damaged by a virus. Sophos can supply utilities for repairing the damage caused by some viruses. Contact Sophos technical support for advice: see *Technical support* (page 20).

6 Appendix A: On-demand scan return codes

sweep returns a code to the shell that indicates the result of the scan. You can view the code by entering a further command after the scan has finished, for example:

echo $?

Return code	Description
0	No errors occur and no viruses are detected
1	The user interrupts the scan by pressing CTRL+C
2	An error occurs that prevents further execution of a scan
3	A virus is detected

6.1 Extended return codes

sweep returns a more detailed code to the shell if you run it with the-**eec** option. You can view the code by entering a further command after the scan has finished, for example:

echo $?

Extended return code	Description
0	No errors occur and no viruses are detected
8	A survivable error occurs
16	A password-protected file is found (it is not scanned)
20	An item containing a virus is detected and disinfected
24	An item containing a virus is found and not disinfected
28	A virus is detected in memory
32	An integrity check failure occurs

Extended return code	Description
36	An unsurvivable error occurs
40	The scan is interrupted

7 Troubleshooting

This section describes how to deal with problems that might arise when usingSophos Anti-Virus.

For information about Sophos Anti-Virus return codes for on-demand scans, see *Appendix A: On-demand scan return codes* (page 13).

7.1 Computer reports “not found”, “No manual entry for sweep”, or “cannot load library”

Symptom

When you try to run **sweep** or view the **sweep** man page, the computer displays a message similar to one of the following:

```
command not found
man page not found
No manual entry for sweep
library not found
cannot load library
```

Cause

This is probably because your environment variables do not include the directories that Sophos Anti-Virus uses.

Resolve the problem

1. If you are running the sh, ksh or bash shell, open /etc/profile for editing.

   If you are running the csh or tcsh shell, open /etc/login for editing.

   Note: If you do not have a login script or profile, carry out the following steps at the command prompt. You must do this every time that you restart the computer.

2. Check that the environment variables include the directories that Sophos Anti-Virus uses:

   PATH should include /usr/local/bin

   MANPATH should include /usr/local/man

   LD_LIBRARY_PATH should include /usr/local/lib

   Note: On AIX, the library environment variable is LIBPATH, and on HP-UX it is SHLIB_PATH.

3. If the environment variables do not include these directories, add them as follows. Do not change any of the existing settings.

   If you are running the sh, ksh or bash shell, type:

PATH=$PATH:/usr/local/bin

export PATH

MANPATH=$MANPATH:/usr/local/man

export MANPATH

LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/lib

export LD_LIBRARY_PATH

If you are running the csh or tcsh shell, type:

setenv PATH *values***:/usr/local/bin**

setenv MANPATH *values***:/usr/local/man**

setenv LD_LIBRARY_PATH *values***:/usr/local/lib**

where *values* are the existing settings.

Note: On some systems, for example FreeBSD and Linux, you can enable Sophos Anti-Virus to use the Sophos Anti-Virus shared libraries by running **ldconfig**. This might require editing of /etc/ld.so.conf.

4. Save the login script or profile.

7.2 Sophos Anti-Virus runs out of disk space

Symptom

Sophos Anti-Virus runs out of disk space, perhaps when scanning complex archives.

Causes

This might be for one of the following reasons:

- When it unpacks archives, Sophos Anti-Virus uses the /tmp directory to store its working results. If this directory is not very large, Sophos Anti-Virus may run out of disk space.
- Sophos Anti-Virus has exceeded the user's quota.

Resolve the problem

Try one of the following:

- Enlarge /tmp.
- Increase the user's quota.
- Change the directory that Sophos Anti-Virus uses for working results. You can do this by setting the environment variable SAV_TMP.

7.3 On-demand scanning runs slowly

This problem may arise for one of the following reasons:

Symptom

Sophos Anti-Virus takes significantly longer to carry out an on-demand scan.

Causes

This might be for one of the following reasons:

- By default, Sophos Anti-Virus performs a quick scan, which scans only the parts of files that are likely to contain viruses. If scanning is set to full (using the option **-f**), it scans the whole file.
- By default, Sophos Anti-Virus scans only particular file types. If it is configured to scan *all* file types, the process takes longer.

Resolve the problem

Try one of the following, as appropriate:

- Avoid using full scanning unless you are advised to, for example by Sophos technical support.
- To scan files that have specific filename extensions, add those extensions to the list of file types that Sophos Anti-Virus scans by default. For more information, see *Scan a particular file type* (page 6).

7.4 Archiver backs up all files that have been scanned on demand

Symptom

Your archiver always backs up all the files that Sophos Anti-Virus has scanned on demand.

Cause

This is because of changes that Sophos Anti-Virus makes in the "status-changed" time of files. By default, Sophos Anti-Virus tries to reset the access time (**atime**) of files to the time shown before scanning. However, this has the effect of changing the inode status-changed time (**ctime**). If your archiver uses the **ctime** to decide whether a file has changed, it backs up all files scanned by Sophos Anti-Virus.

Resolve the problem

Run **sweep** with the option **--no-reset-atime**.

7.5 Virus not cleaned up

Symptoms

- Sophos Anti-Virus has not attempted to clean up a virus.
- Sophos Anti-Virus displays `Disinfection failed`.

Causes

This might be for one of the following reasons:

- Automatic cleanup has not been enabled.
- Sophos Anti-Virus cannot disinfect that type of virus.
- The infected file is on a removable medium, for example floppy disk or CD, that is write-protected.
- The infected file is on an NTFS filesystem.
- Sophos Anti-Virus does not clean up a virus fragment because it has not found an exact virus match.

Resolve the problem

Try one of the following, as appropriate:

- Enable automatic cleanup.
- If possible, make the removable medium writeable.
- Deal with files that are on an NTFS filesystem on the local computer instead.

7.6 Virus fragment reported

Symptom

Sophos Anti-Virus reports that it has detected a virus fragment.

Causes

This indicates that part of a file matches part of a virus. This is for one of the following reasons:

- Many new viruses are based on existing ones. Therefore, code fragments that are typical of a known virus might appear in files that are infected with a new one.
- Many viruses contain bugs in their replication routines that cause them to infect target files incorrectly. An inactive part of the virus (possibly a substantial part) may appear in the host file, and this is detected by Sophos Anti-Virus.
- When running a full scan, Sophos Anti-Virus may report that there is a virus fragment in a database file.

Resolve the problem

1. Update Sophos Anti-Virus on the affected computer so that it has the latest virus data.
2. Try to disinfect the file: see *Disinfect a specific infected file* (page 11).
3. If virus fragments are still reported, contact Sophos technical support for advice: see *Technical support* (page 20).

8 Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the SophosTalk community at *http://community.sophos.com/* and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at *http://www.sophos.com/support/*.
- Download the product documentation at *http://www.sophos.com/support/docs/*.
- Send an email to *support@sophos.com*, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

9 Legal notices

Copyright © 2002–2011 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Limited. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

Index

A

alerts
    command-line 9
analyses of viruses 10
archives
    on-demand scans 6, 7

B

backups of scanned files 17
boot sectors
    disinfecting 12
    on-demand scans 5

C

cannot load library 15
cleaning up infected files 11
cleanup information 10
CLI (command-line interface) 4
command not found 15
command-line alerts 9
command-line interface (CLI) 4
computer, on-demand scans 5

D

deleting infected files 12
directories, on-demand scans 5
disinfecting
    boot sectors 12
    infected files 11
disk space insufficient 16

E

error codes 13
excluding items
    on-demand scans 8

F

file types, on-demand scans 6, 8
files, on-demand scans 5
filesystems, on-demand scans 5, 7
fragment reported, viruses 18

I

infected files
    cleaning up 11
    deleting 12
    disinfecting 11
    quarantining 10

L

library not found 15

M

man page not found 15

N

No manual entry for sweep 15

O

on-demand scans 5
    archives 6, 7
    boot sectors 5
    computer 5
    directories 5
    excluding items 8
    file types 6, 8
    files 5
    filesystems 5, 7
    remote computers 7
    symbolically linked items 7
    UNIX executables 8

Q

quarantining infected files 10

R

remote computers, on-demand scans 7
return codes 13

S

side-effects of viruses 12
slow on-demand scans 17
symbolically linked items, on-demand scans 7

U

UNIX executables, on-demand scans 8

V

viruses
- analyses 10
- detected 9
- fragment reported 18
- not cleaned up 18
- side-effects 12